JAY EDELSON (Admitted *Pro Hac Vice*)
(jedelson@edelson.com)
RAFEY S. BALABANIAN (Admitted *Pro Hac Vice*)
(rbalabanian@edelson.com)
ARI J. SCHARG (Admitted *Pro Hac Vice*)
(ascharg@edelson.com)
CHRISTOPHER L. DORE (Admitted *Pro Hac Vice*)
(cdore@edelson.com)
EDELSON LLC
350 North LaSalle, Suite 1300
Chicago, Illinois 60654
Tel: (312) 589-6370

LAURENCE D. KING (SBN 206423)
(lking@kaplanfox.com)
LINDA M. FONG (SBN 124232)
(lfong@kaplanfox.com)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, California 94104
Tel: (415) 772-4700

[Additional counsel appear on the signature page.]

Counsel for Plaintiff and the Putative Class

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE LINKEDIN USER PRIVACY LITIGATION	Case No. 12-cv-03088-EJD **SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT FOR:** **(1) Violations of Cal. Bus. & Prof. Code §§ 17200, *et seq.*; and** **(2) Breach of Contract.** **DEMAND FOR JURY TRIAL**

Plaintiff Khalilah Wright ("Plaintiff" or "Wright"), by and through her attorneys, upon personal knowledge as to herself and her own acts and experiences including through investigation conducted by her attorneys, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff Wright brings this Second Amended Consolidated Class Action Complaint ("Complaint") against Defendant LinkedIn Corporation ("LinkedIn") to remedy LinkedIn's decision to dupe its customers into paying for services, and then supplying them with entirely different, less useful, and less valuable services instead.

2. LinkedIn owns and operates the website www.LinkedIn.com, a social networking website with over 200 million registered users that bills itself as the "World's Largest Professional Network."

3. When signing up for LinkedIn's services, users build personal "profiles" by providing LinkedIn with various types of demographic, occupational, and cultural information, including employment and educational history.

4. Among its services, LinkedIn sells Premium Subscriptions, which provide enhanced features and functionality compared to its "free" services. In order to purchase its Premium Subscriptions, LinkedIn's customers must provide their credit card and billing information to LinkedIn, and then pay LinkedIn subscription fees ranging from $19.95 to $499.95 per month.

5. As part of their purchases of the Premium Subscriptions, reasonable consumers—including Plaintiff Wright—expect and are entitled to have their personal and financial information protected by industry-standard data and information security practices.

6. When a LinkedIn customer purchases a LinkedIn Premium Subscription, the customer is required to agree to a contract governing his or her use, and LinkedIn's provision of, the Premium Subscription. This contract incorporates by reference LinkedIn's Privacy Policy,

"which governs our treatment of any information, including personally identifiable information you submit to us." The contract further states "that [it] constitutes the entire, complete and exclusive agreement between [the user] and [LinkedIn] regarding the Services and supersedes all prior agreements and understandings . . . ."[1]

7. As part of these new contracts for Premium Subscriptions, LinkedIn promises to use industry-standard technologies and procedures to protect its Premium Subscribers' personal information.

8. Thus, when customers like Wright purchase Premium Subscriptions, they do not merely purchase access to additional features and functionality. Rather, they purchase an indivisible bundle of Premium Services, including LinkedIn's social and professional networking services, as well as industry-standard data privacy and security services as set forth in LinkedIn's Privacy Policy, which is incorporated into the new contract governing the Premium Subscriptions.

9. Unfortunately for its consumers, LinkedIn did not—despite its users' expectations, and its own promises, to the contrary—utilize industry-standard measures to protect its customers' sensitive personal data. Instead, and despite its reputation as a leading consumer data management company, LinkedIn used data security measures that have been outdated since at least 2006.

10. Had LinkedIn informed its Premium Subscribers that it would use security measures that were obsolete before the iPhone or Twitter were first released, Wright would not have been willing to purchase her LinkedIn Premium Subscription at the price charged, if at all.

11. Thus, because LinkedIn failed to disclose its gross security inadequacies to Plaintiff and the Class, it delivered to Plaintiff and the Class a fundamentally less useful and less valuable service than the one they paid for. Accordingly, Plaintiff Khalilah Wright brings suit on

[1] *LinkedIn Terms of Service*, LinkedIn.com, http://www.linkedin.com/static?key=pop%2Fpop_multi_currency_user_agreement&type=sub (last accessed Apr. 30, 2013).

behalf of herself and all others similarly situated, to seek redress for LinkedIn's deceptive and unlawful conduct.

PARTIES

12. Plaintiff Khalilah Wright is a natural person and resident of the State of Virginia. Wright is a registered user of LinkedIn's services and had a Premium Subscription from March 2010 to approximately August 2010.

13. Defendant LinkedIn Corporation is a corporation incorporated in and existing under the laws of the State of Delaware, with its principal place of business located at 2029 Stierlin Court, Mountain View, California 94043. LinkedIn does business throughout this District, the State of California, and the United States.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because (a) at least one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (c) none of the exceptions under the subsection apply to this action.

15. This Court has personal jurisdiction over Defendant because it is headquartered in this District, conducts significant business in this District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated from this District.

16. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant maintains its headquarters and principal place of business in this District and a substantial part of the events giving rise to Plaintiff's Complaint occurred in this District.

FACTUAL BACKGROUND

LinkedIn Sells A Bundle Of Premium Services To The Class Members.

17. LinkedIn claims that it "operates the world's largest professional network on the Internet with more than 200 million members in over 200 countries and territories."[2]

[2] *About LinkedIn*, LinkedIn, http://press.linkedin.com/about (last visited Apr. 30, 2013).

18. A customer may sign up for a membership at www.LinkedIn.com by providing LinkedIn with a valid e-mail address and a registration password. LinkedIn then stores these credentials in databases located on its servers. Once registered, users build personal "profiles" by providing LinkedIn with various types of demographic, occupational, and cultural information, including employment and educational history.

19. LinkedIn offers its customers the ability to purchase LinkedIn Premium Subscriptions, which require customers to provide additional credit card and billing information. These Premium Subscriptions include enhanced social networking features, messaging options, search results, organizational tools, industry-standard security practices, and more, for prices ranging from $19.95 to $499.95 per month, depending on the features and the plan chosen.

20. When a customer agrees to purchase a LinkedIn Premium Subscription, the user must provide credit card and billing information and agree to a new contract, which, by its own terms "constitutes the entire, complete and exclusive agreement between [the user] and [LinkedIn] regarding the Services and supersedes all prior agreements and understandings."[3] In other words, when a customer signs up for a LinkedIn Premium Subscription, that customer is not merely purchasing add-ons to the existing LinkedIn service. Instead, the customer is cancelling the original basic LinkedIn contract and entering into a new contract with LinkedIn, whereby, in exchange for the monthly subscription fee paid by the user, LinkedIn will provide a bundle of services, including the basic social networking features, premium features, and industry-standard data privacy and security measures.

21. Together, the features LinkedIn Premium Subscribers paid for—the basic features, the additional premium features, and the industry-standard security protections—have a value greater than the sum of their parts. That is, the utility of the bundle of services offered in a LinkedIn Premium Subscription is greater than the combined utility of the individual

[3] *LinkedIn Terms of Service*, LinkedIn, http://www.linkedin.com/static?key=pop%2Fpop_multi_currency_user_agreement&type=sub (last accessed Apr. 30, 2013).

components (*i.e.*, base features, premium features, and privacy and security measures).

22. Accordingly, as the number of features offered (and data collected) increases from the LinkedIn basic account to the LinkedIn Premium Subscription, industry-standard security measures become of ever-increasing importance, and their utility and value to the bundle of services increases.

23. Thus, as detailed more fully below, if LinkedIn had revealed that its Premium Subscriptions did not include industry-standard security practices and protocols for their personal and financial information, the Premium Subscription would have been viewed as having substantially lower value and utility, and LinkedIn could not have charged the prices it did for those Premium Subscriptions.

As Part Of Their Premium Subscriptions, LinkedIn's Customers Justifiably Expected To Receive Industry-Standard Protections And Security For Their Personal Information.

24. As part of their purchases of the LinkedIn Premium Subscriptions, Wright and the Class expected that they would, at a minimum, receive industry-standard security protections for their personal information and data stored by LinkedIn.

25. As part of the investigation into her case, Wright retained Dr. Serge Egelman, one of the nation's leading experts on the behavioral economics of data privacy and security, to investigate consumers' privacy and security expectations when paying for a social networking service. (A true and accurate copy of Dr. Egelman's Expert Report ("Egelman Rep.") is attached hereto as Exhibit A-2.)

26. Through his investigation, Dr. Egelman found that when consumers pay for a social networking service, they expect a heightened level of security, and, "[t]hey expected that part of their subscription fee was going towards the secure storage of their personal information using practices that met or exceeded industry standards." (Egelman Rep. at 3.)

27. These minimal expectations are both reasonable and justified when applied to LinkedIn for several reasons. First, as a "company that collects and profits from vast amounts of

data," "customers and security experts alike" expect LinkedIn to at least keep up with industry standard security measures for that data.[4]

28. Second and more importantly, LinkedIn itself justifies its customers' expectations by promising consumers exactly what they expect as part of their Premium Subscriptions. In LinkedIn's Privacy Policy, which is incorporated into the Terms of Service governing the Premium Subscriptions, LinkedIn promises its users that "[a]ll information that you provide will be protected with industry standard protocols and technology."[5]

29. Accordingly, as part of their Premium Subscriptions, Plaintiff and the Class members reasonably and justifiably expected that the personal information they provided to LinkedIn would be protected using industry-standard security protocols.

LinkedIn Fails To Deliver The Security Its Customers Expect.

30. Within the consumer technology services sector, industry standards dictate that users' personal information, including login credentials (usernames and passwords), be stored in an encrypted rather than plain-text format.

31. Since at least 2006, industry standards have required that users' personal information, and login credentials in particular, be stored in salted and hashed format.

32. Salting and hashing is a two-step process. First, the information to be protected is "salted" by "concatenating a plaintext password with a series of randomly generated characters prior to hashing." (Egelman Rep. at 13 – 14.)

33. Second, the salted password (or other information) is "hashed." A password or other information is "hashed" by applying a one-way function or algorithm to it. "Hash functions are designed to reveal no information about the underlying input" (the password or other

[4] *See* Nicole Perlroth, *Lax Security at LinkedIn is Laid Bare*, N.Y. Times (June 10, 2012), *available at* http://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html?pagewanted=all&_r=0.

[5] *Privacy Policy*, LinkedIn, http://www.linkedin.com/legal/privacy-policy (last accessed Apr. 30, 2013).

information), and are designed such that minor changes in inputs will result in major changes to outputs. (*Id.* at 11 – 13.)

34. While hashing alone does encrypt information and offer some degree of security, hashing using the SHA-1 algorithm (as used by LinkedIn) is vulnerable to hacking through a variety of specialized tools, publicly available cloud-computing platforms such as Amazon's EC2 or Microsoft's Azure, and common commodity hardware. SHA-1 hashing is also particularly susceptible to hacking through the use of "rainbow tables," which are "list[s] of input strings and their resulting hashes that have been precomputed, in order to save someone the time of computing the hashes themselves." (*Id*. at 13.)

35. Because of these vulnerabilities, in 2006, the National Institute of Standards and Technology recommended that all governmental agencies "stop using SHA-1 for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical."[6]

36. Salting (used in addition to hashing), however, has the advantage of rendering inoperative several commonly available methods for "cracking" passwords or other information stored in hashed-only format. (Egelman Rep. at 13 – 14.) For this reason, salting has been standard encryption practice since the 1970s, and salting and hashing (with a stronger algorithm than SHA-1) together is the preferred industry practice. (*Id.* at 11, 14.)

37. On June 6, 2012, a list of approximately 6.4 million hashed LinkedIn user passwords were posted online. Reports indicated that LinkedIn's servers were breached through a common hacking method known as an "SQL injection" attack. This hacking technique involves exploiting weaknesses existing in a company's website to penetrate deeper into back-end servers that house databases of sensitive user information.

38. LinkedIn was not even aware that its systems had been hacked, and its customers' personal information compromised, until after its users' passwords were posted online.

[6] *NIST's March 2006 Policy on Hash Functions*, National Institute of Standards and Technology (Sept. 24, 2012), http://csrc.nist.gov/groups/ST/hash/policy_2006.html.

39. When the 6.4 million LinkedIn user passwords were posted online, it was revealed that LinkedIn had been storing its users' passwords using unsalted, SHA-1 hashed encryption.

40. Three days after the breach, LinkedIn confirmed that it was not handling user data in accordance with best practices. LinkedIn stated that "one of our major initiatives was the transition from a password database system that hashed passwords, i.e. provided one layer of encoding, to a system that both hashed and salted the passwords, i.e. provided an extra layer of protection *that is a widely recognized best practice within the industry*. That transition was completed prior to news of the password theft breaking on Wednesday. We continue to execute on our security roadmap, and we'll be releasing additional enhancements to better protect our members."[7] But these actions were too little too late—LinkedIn's transition to industry-standard data protection practices clearly occurred *after* its servers were breached, as the passwords publicly posted were, by its own admission, only hashed.

41. Thus, by using bare SHA-1 hashing without salting, LinkedIn employed an easily compromised encryption algorithm that had been abandoned for government use in 2006.

42. Indeed, because LinkedIn only used SHA-1 hashing and did not salt its users' passwords, the majority of the publicly posted hashed passwords were decoded within days, and at least one industry expert estimated that 95 percent of the passwords would be cracked.[8]

43. The bare minimum practice within LinkedIn's industry is to "salt" the input before hashing it, preferably with a multi-digit salt long enough to render rainbow tables entirely useless. (Egelman Rep. at 14.)

44. Indeed, the more common industry practice is to (1) salt passwords and then hash them using a more recent and secure algorithm than SHA-1, (2) salt the resulting hash value, and

---

[7] Vincente Silveira, *An Update On Taking Steps To Protect Our Members*, LinkedIn Blog (June 9, 2012), http://blog.linkedin.com/2012/06/09/an-update-on-taking-steps-to-protect-our-members/ (emphasis added).

[8] *See* Perlroth, *supra* note 4.

(3) then again run the resulting value through a hashing function. Finally, that fully encrypted password should be stored on a separate and secure server apart from all other user information.

45. LinkedIn, by its own admission, however, did not use these industry-standard protections for its users' personal information. Instead, LinkedIn used an easily-cracked encryption algorithm abandoned by government agencies more than 6 years prior, and then failed to secure its website—and, more importantly, its users' information stored on its back-end servers—from a relatively common SQL injection attack.

46. LinkedIn's failure to protect its website against common SQL injection attacks, in conjunction with storing its users' personal information in SHA-1 hashed, unsalted format, demonstrates that LinkedIn failed to use industry-standard security to protect its users' personal information.

Had LinkedIn Disclosed Its True Security Practices, The Class Members Would Have Learned Of Them.

47. Companies like LinkedIn put information in their privacy policies to inform customers of their data practices.

48. Consumers typically learn of the contents of privacy policies in two ways. First, they learn directly, by reading the policies. Second, consumers learn indirectly, through word of mouth and popular media.

49. As to indirect learning, when privacy policies are changed, they are typically read and analyzed by a relatively small group of experts, who then inform others and the media when a particular policy greatly diverges from industry standards. (*See* Egelman Rep. at 16 – 17.) Through popular media accounts and word of mouth from acquaintances, website users learn even more detail about the privacy policy changes and their effects.

50. For instance, research has shown that when Facebook, the world's largest social network, changes its privacy policy, users learn of the changes through word of mouth, popular media accounts, and knowledge gained by prior interactions, despite the complexity of

Facebook's privacy policy and the potentially subtle nature of changes to it. (*See id*. at 17.)

51. Likewise, in 2012, the popular photo-sharing social network Instagram changed its privacy policy to include a clause stating that users' photos could be used for advertising purposes. Despite the high level of complexity found in Instagram's privacy policy, the popular media quickly noted the change to the privacy policy, and users—informed by popular media accounts—expressed their displeasure. Concerned with the possibility of losing users, Instagram ended up removing the offending clause. (*See id*. at 16 – 17.)

52. In the Privacy Policy governing the Premium Subscriptions, LinkedIn represented that it used industry-standard security protocols to protect its customers' personal information. This representation, along with the nature of its business and its standing within its industry, led consumers, experts, and market participants to believe that LinkedIn did, in fact, use industry-standard data protection measures.

53. Had LinkedIn disclosed that it was only using unsalted SHA-1 encryption to protect users' data, its users would have found out. In the wake of the LinkedIn passwords being posted online, the popular media coverage of the breach focused not on the relatively commonplace occurrence of a website hack, but rather on the fact that LinkedIn's security practices fell so far below industry standards. (*See id.* at 15 (containing relevant media quotes regarding LinkedIn's deficient security).)

54. Had LinkedIn's security practices been publicized through its own disclosures (rather than through a hack), the response would likely still have been emphatic, as the lack of a breach would do nothing to make LinkedIn's disregard for industry standards any less remarkable.

55. Thus, through both direct (first-hand) and indirect experience, had LinkedIn disclosed its decision to use SHA-1 unsalted encryption, its Premium Subscribers would have known that LinkedIn used substandard security practices.

LinkedIn's Failure To Disclose Its True Security Practices Caused Class Members To Receive Less Useful Services Than Those They Paid For.

56. Consumers place value in data privacy and security, and they consider it in making purchasing decisions.

57. Further, "it is widely known among businesses that consumers are willing to pay increased prices in order to do business with merchants who better protect their privacy by following" FTC best practices. (*Id*. at 5.) In fact, little "research has been performed since 2004 to establish *whether* people value privacy, since it is widely understood that they do. Research has since shifted to examine the extent to which they value it, when balanced with other concerns, and how this changes based on specific circumstances." (*Id.* at 4 n.1) (emphasis added).[9]

58. Academic research has shown that consumers are willing to spend additional money (a premium) in exchange for "stronger privacy protections, which includes the secure storage of their personal information," and research also supports the corollary point, that consumers expect increased data security and privacy when they pay additional money for a service. (*Id.* at 5 – 6.)

59. Consumer software and technology markets have likewise demonstrated that consumers value their privacy and security and incorporate data security practices into their purchases. For example, companies have emerged providing consumers with "cloaking services," that allow consumers to browse the Internet anonymously for a $30 to $40 premium.[10] Likewise, companies now offer services that, in exchange for a monthly fee, will offer online

[9] *See also* Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Apr. 30, 2013) ("The real policy issue is not whether consumers value online privacy. It is obvious that people value online privacy.").

[10] *See* Rust et al., *The Customer Economics of Internet Privacy*, Journal of the Academy of Marketing Sciences 30, 4 (2002) at 461.

services designed to protect data privacy.[11]

60. Consumers are especially eager to ensure the security of their login credentials (usernames and passwords), leading to the development of a market where consumers can buy software and services to securely store and manage the usernames and passwords they use on various websites.[12]

61. Because of the value consumers place on data privacy and security, services with better security practices command higher prices than those without. Indeed, if consumers did not value their data security and privacy, profit-seeking corporations (like LinkedIn) would have no reason to tout their privacy and security credentials to current and prospective customers.

62. These value propositions reflect the fact that consumers view social networking services with industry-standard security protections as being far more useful than those with substandard protections, which users view as "not at all useful." (Egelman Rep. at 9.)

63. Likewise, across all price ranges, users are more willing to pay for social networking services that offer industry-standard security than social networks with substandard security. Further, when calculating the utility of social networking websites, consumers factor stated security practices heavily into their calculations. (*Id*. at 10 – 11.)

64. As a result of those concerns and the value placed on security, consumers simply believe that a social network that costs money but does not offer at least industry-standard security is not worth paying for or using. (*Id*. at 10 – 11.) Research shows that consumers do not view unsecure social networking websites as substitutes for secure social networks.

---

[11] *See Simple pricing, advanced service*, Safe Shepherd, https://www.safeshepherd.com/pricing (last accessed Apr. 30, 2013) (offering basic privacy protection services for free, an advanced service for $13.95 per month, and a "VIP" service for $249.95 per month); *see also Identity Protection Software*, Norton by Symantec, http://buy.norton.com/en-us/identity-protection-software (last accessed Apr. 30, 2013).

[12] *See Kapersky Password Manager*, Kapersky Lab, http://usa.kaspersky.com/products-services/home-computer-security/password-manager?domain=kaspersky.com (last accessed Apr. 30, 2013); *see also* Neil J. Rubenking, *Six Great Password Managers*, PCMag.com (Mar. 11, 2011), http://www.pcmag.com/article2/0,2817,2381432,00.asp.

65. As a result, a social networking service with substandard data security and privacy protections is objectively less useful and valuable than a social networking service with industry-standard security protocols, and is, in reality, a different service entirely.

FACTS RELATING TO PLAINTIFF KHALILAH WRIGHT

66. Plaintiff Wright paid for a LinkedIn Premium Subscription from March 2010 until approximately August 2010.

67. Before signing up for her LinkedIn Premium Subscription, Wright—as she always does when signing up for a service online—read and agreed to the Terms of Service and Privacy Policy and the representations and obligations listed therein.

68. The Terms of Service governing Wright's LinkedIn Premium Subscription specifically stated that "this Agreement constitutes the entire, complete and exclusive agreement between you and us regarding the Services and supersedes all prior agreements and understandings, whether written or oral, or whether established by custom, practice, policy or precedent, with respect to the subject matter of this Agreement."[13]

69. The Terms of Service governing Wright's LinkedIn Premium Subscription also "incorporated by reference" LinkedIn's Privacy Policy, and advised her to "[r]eview and comply with [LinkedIn's] Privacy Policy."[14]

70. Following her normal routine, Wright also read LinkedIn's Privacy Policy and the representations contained therein before agreeing to purchase a LinkedIn Premium Subscription. In its Privacy Policy, LinkedIn promised Wright that the "[p]ersonal information you provide will be secured in accordance with industry standards and technology."[15]

71. Because she was signing up for a paid social networking service, Wright believed that LinkedIn would use reasonable and accepted methods of securing her personal information,

---

[13] *See LinkedIn Terms of Service*, *supra* note 3.

[14] *Id.*

[15] *See Privacy Policy*, *supra* note 5.

and LinkedIn confirmed that belief with the representations in its Privacy Policy.

72. Accordingly, when Wright cancelled her basic LinkedIn contract and initiated her LinkedIn Premium Subscription, she paid a monthly fee for the combination of LinkedIn's basic features, its premium features, and industry-standard privacy and security measures for protecting her personal information.

73. The three components to her purchase—the basic features, the premium features, and the security—combined to establish the valuable service Wright paid for. Thus, without the industry-standard security protections Wright justifiably believed she was entitled to as part of her purchase, the LinkedIn Premium Subscription as a whole was substantially less useful and valuable to her.

74. In fact, to Wright, a secure Premium Subscription is a fundamentally different service than an unsecure Premium Subscription, and an unsecure Premium Subscription would not be an adequate or comparable replacement for a secure Premium Subscription.

75. Had LinkedIn disclosed that it was using security protocols disavowed by government agencies since 2006, Wright would—through reading the Privacy Policy and/or through the popular media—have been aware of those disclosures.

76. Accordingly, had LinkedIn disclosed its lax security practices, she would have viewed the Premium Subscription as less valuable and would either have attempted to purchase a Premium Subscription at a lower price or not at all.

CLASS ALLEGATIONS

77. Plaintiff Khalilah Wright brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of herself and a Class of similarly situated individuals, defined as:

> All individuals and entities in the United States who paid a monthly fee to LinkedIn for a Premium Subscription at any point between March 15, 2006 and June 7, 2012.

Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and

any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) counsel for Plaintiff and Defendant; (4) persons who properly execute and file a timely request for exclusion from the class; (5) the legal representatives, successors or assigns of any such excluded persons; (6) all persons who have previously had claims similar to those alleged herein finally adjudicated or who have released their claims against Defendant; and (7) any individual who contributed to the unauthorized access of Defendant's database.

78. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but on information and belief, there are millions of people in the Class, making joinder of each individual member impracticable. Ultimately, members of the Class will be easily identified through Defendant's records.

79. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include but are not limited to the following:

(a) whether LinkedIn failed to protect users' PII with industry-standard protocols and technology;

(b) whether LinkedIn's conduct described herein violates California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq*.); and

(c) whether LinkedIn's conduct described herein constitutes a breach of contract.

80. **Typicality**: Plaintiff's claims are typical of the claims of all the other members of the Class. Plaintiff and the Class members sustained substantially similar damages as a result of Defendant's uniform wrongful conduct, based upon the same transactions that were made uniformly with Plaintiff and the public.

81. **Adequate Representation**: Plaintiff will fairly and adequately represent and

protect the interests of the other members of the Class. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

82. **Policies Generally Applicable to the Class**: Defendant has acted and failed to act on grounds generally applicable to Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class.

83. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered and uniformity of decisions ensured.

84. Plaintiff reserves the right to revise the Class Definition and Class Allegations based on further investigation, including facts learned in discovery.

//

//

//

FIRST CAUSE OF ACTION
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiff and the Class)

85. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

86. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq*., protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

87. The UCL prohibits any unlawful, unfair, or fraudulent business act or practice. A business practice need only meet one of the three criteria to be considered unfair competition. A deceptive business practice is one that is likely to deceive members of the public.

88. When consumers pay for a social networking service, they expect that the service will provide, at a bare minimum, industry-standard security protections for their personal information. (Egelman Rep. at 3.)

89. Thus, when Plaintiff Wright and the Class paid for their LinkedIn Premium Subscriptions, they expected LinkedIn to protect their personal information—including their usernames and passwords—with industry-standard security protocols.

90. Wright's and the Class's expectation was justified by the fact that LinkedIn promised in the Terms of Service governing the Premium Subscriptions to use industry-standard methods to protect their personal information.

91. By maintaining its Premium Subscribers' personal information in SHA-1 unsalted format, LinkedIn used security that has been outdated since at least 2006, and failed to employ salting measures that have been standard security practice since the 1970s. Thus, LinkedIn did not use industry-standard security protocols to protect Wright's and the Class's personal information. (*See* Egelman Rep. at 14 – 15.)

//

//

//

92. In fact, LinkedIn's security protocols were such a material deviation from industry standards that their noncompliance—when finally revealed by the breach—was newsworthy in and of itself. (*See id.* at 15.)[16]

93. LinkedIn was responsible for securing its Premium Subscribers' personal information. As part of its own data management, LinkedIn knew that it was using unsalted SHA-1 encryption to safeguard its customers' data rather than industry-standard practices. Prior to the breach, neither LinkedIn's Premium Subscribers nor the general public knew that LinkedIn was using such outdated security protocols. Further still, by representing that it used industry-standard security protocols, when it did not in fact do so, LinkedIn actively concealed its true security practices from Wright and the Class.

94. LinkedIn touted itself as a leading Internet services company, its users expected that as part of their Premium Subscriptions they would be entitled to—at a bare minimum—industry-standard security practices, and LinkedIn represented that it did in fact provide industry-standard security measures for its users' personal information. Accordingly, LinkedIn's decision to omit the truth about its security practices—that it used obsolete security methods disavowed by government agencies almost a decade ago—was a material deviation from its Premium Subscribers' expectations and was therefore likely to deceive the public.

95. Because LinkedIn's outdated security practices were newsworthy on their own, had LinkedIn disclosed its substandard security practices prior to the breach, Wright and the

[16] *See also* Brian Krebs, *How Companies Can Beef Up Password Security*, Krebs on Security (June 11, 2012), http://krebsonsecurity.com/2012/06/how-companies-can-beef-up-password-security/; Dan Rowinski, *Avoiding Password Breaches 101: Salt Your Hash*, ReadWrite (June 7, 2012), http://readwrite.com/2012/06/07/avoiding-password-breaches-101-salt-your-hash; Elinor Mills, *LinkedIn confirms passwords were 'compromised,'* CNET (June 6, 2012), http://news.cnet.com/8301-1009_3-57448465-83/linkedin-confirms-passwords-were-compromised/; Michael Hickins, *LinkedIn Password Breach Illustrates Endemic Security Issue*, CIO Journal (June 6, 2012), http://blogs.wsj.com/cio/2012/06/06/linkedin-password-breach-illustrates-endemic-security-issue/; Perlroth, *supra* note 4; Paul Hartsock, *LinkedIn: Unsalted, Assaulted and Faulted*, TechNewsWorld (June 9, 2012), http://www.technewsworld.com/story/75337.html; Poul-Henning Kamp, *LinkedIn Password Leak: Salt Their Hide*, ACM Queue (June 7, 2012), http://queue.acm.org/detail.cfm?id=2254400.

Class would have known of those disclosures (and thus, of LinkedIn's true security practices), through word of mouth, popular media coverage, and (if disclosed there) reading LinkedIn's Privacy Policy. (*See* Egelman Rep. at 16 – 17); *see also* note 16 *supra*.

96. Consumers, including social network users, value their privacy. Services, including social networking services, that offer greater data security protections are of greater usefulness and utility to consumers than services with substandard security practices. As such, consumers will, if given the choice between two otherwise identical services, choose one with industry-standard security practices over one with substandard security practices.

97. Because of this consumer preference for data security, a social network service with industry-standard security protocols commands a higher market price than a social network service with substandard security.

98. Wright and the Class believed they would receive industry-standard protection for their personal information as part of their LinkedIn Premium Subscriptions, those security protections were valuable to them, and the protections formed the basis of the bargain inasmuch as Wright and the Class would not have purchased their Premium Subscriptions at the prices charged had LinkedIn disclosed its substandard security practices. Accordingly, LinkedIn's omission regarding the true protection standard was material.

99. To Wright and the Class, the as-promised LinkedIn Premium Subscription offers significantly more utility than the service delivered, which lacked meaningful security protections. Thus, to Wright and the Class, the LinkedIn Premium Subscriptions promised and paid-for were substantially more valuable than the unsecure services received.

100. At the same price point, Wright and the Class would purchase the LinkedIn Premium Subscription as-promised instead of the unsecure service they actually received.

101. Accordingly, had Wright and the Class known that LinkedIn did *not* offer industry-standard security protections as part of its Premium Subscriptions, they would not have been willing to purchase the subscriptions at the prices LinkedIn charged for the allegedly secure

Premium Subscriptions, if they would have paid money at all.

102. LinkedIn's failure to disclose its substandard security practices substantially injured the public because it caused millions of consumers to enter into transactions they otherwise would not have, and because it compromised the integrity of the Class members' personal information. Further, LinkedIn's use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

103. Pursuant to Cal. Bus. & Prof. Code §§ 17203 and/or 17204, Plaintiff Wright seeks an order requiring Defendant to: (1) immediately stop the unlawful practices described in this Complaint; (2) ensure that LinkedIn employs commercially reasonable methods to safeguard its user data; (3) provide restitution to Plaintiff and the Class in an amount equal to the difference in value between the services paid for and the services delivered; and (4) pay attorney's fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

SECOND CAUSE OF ACTION
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiff and the Class)

104. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

105. California's UCL protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

106. The UCL prohibits any unlawful, unfair, or fraudulent business act or practice. A business practice need only meet one of the three criteria to be considered unfair competition. An unlawful business practice is one that violates a federal, state, or local law. An unfair business practice is one which offends an established public policy or is otherwise immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.

107. California's Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22576 ("OPPA"), prohibits any company whose website collects personally identifiable information from California consumers from "knowingly and willfully" or "negligently and materially"

breaching its own posted privacy policy.

108. LinkedIn owns and operates the LinkedIn Premium Subscription online service.

109. Through the LinkedIn Premium service, LinkedIn collects personally identifiable information such as name, e-mail address, phone number, education and employment background, credit card payment information, and more from California residents.

110. LinkedIn's Premium Service has a posted Privacy Policy.

111. The posted Privacy Policy for LinkedIn's Premium Service promises that LinkedIn will safeguard its users' personal information "in accordance with industry standards and technology."[17]

112. By storing its Premium Subscribers' login credentials in unsalted, SHA-1 hashed format, LinkedIn did not store its users' personal information "in accordance with industry standards and technology."

113. LinkedIn, a leading online services company and the world's largest professional social network, claims to work with TRUSTe, a data privacy management organization, to ensure its data usage policies comply with industry standards and regulations. This, along with the very fact that it claims to use industry-standard security protocols, demonstrates that LinkedIn knows what industry-standard security protocols entail.

114. LinkedIn made the deliberate decision to use unsalted SHA-1 encryption to protect the Class members' personal information. Thus, LinkedIn knew what its security protocols were, and it knew that they were below industry standards.

115. Accordingly, given LinkedIn's knowledge of industry standards and its intentional decision to use substandard security, its noncompliance with its own privacy policy was both knowing and willful.

116. If nothing else, LinkedIn should reasonably have known that its security practices did not meet industry standards. Accordingly, as shown by the popular media response to

[17] *Privacy Policy*, *supra* note 5.

LinkedIn's substandard security practices and the research showing that consumers do incorporate security and privacy concerns into purchasing decisions, LinkedIn's noncompliance with its own privacy policy was—at a bare minimum—negligent and material.

117. Because it violated OPPA, LinkedIn's noncompliance with its own posted privacy policy is an unlawful business practice under the UCL.

118. Further, as detailed in Count III below, Defendant's conduct described herein constitutes a systematic and material breach of its contracts with Wright and each of the Class Members. As such, Defendant's systematic breach constitutes unlawful and unfair conduct in violation of the UCL.

119. Consumers, including social network users, value their privacy. Services, including social networking services, that offer greater data security protections are of greater usefulness and utility to consumers than services with substandard security practices. As such, consumers will, if given the choice between two otherwise identical services, choose one with industry-standard security practices over one with substandard security practices.

120. Wright and the Class believed they would receive industry-standard protection for their personal information as part of their LinkedIn Premium Subscriptions, and those security protections were valuable to them.

121. Consumers, including social network users, value their privacy. Services, including social networking services, that offer greater data security protections offer consumers greater usefulness and utility than services with substandard security practices. As such, consumers will, if given the choice between two otherwise identical services, choose one with industry-standard security practices over one with substandard security practices.

122. Because of this consumer preference for data security, a social network service with industry-standard security protocols commands a higher market price than a social network service with substandard security protocols.

123. To Wright and the Class, the as-promised LinkedIn Premium Subscription offered

significantly more utility than the service delivered, which lacked meaningful security protections. Thus, to Wright and the Class, the LinkedIn Premium Subscriptions promised and paid-for were substantially more valuable than the unsecure services they received instead.

124. At the same price point, Wright and the Class would have purchased the LinkedIn Premium Subscription as-promised instead of the unsecure service they actually received.

125. Accordingly, had Wright and the Class known that LinkedIn did *not* offer industry-standard security protections as part of its Premium Subscriptions, they would not have been willing to purchase the subscriptions at the prices LinkedIn charged for the allegedly secure Premium Subscriptions, if they would have paid money at all.

126. As a result of LinkedIn's substandard security practices, while Wright and the Class held up their end of the bargain by paying their subscription fees and abiding by the Terms of Service, they received a service (the actual LinkedIn Premium Subscription) that was substantially less useful and worth less to them than the one they paid for (the Premium Subscription, as promised), which would have included industry-standard security protections.

127. LinkedIn's failure to disclose its substandard security practices substantially injured the public because it caused millions of consumers to enter into transactions they otherwise would not have, and because it compromised the integrity of the Class members' personal information. Further, LinkedIn's use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

128. Pursuant to Cal. Bus. & Prof. Code §§ 17203 and/or 17204, Plaintiff Wright seeks an order requiring Defendant to: (1) immediately stop the unlawful practices described in this Complaint; (2) ensure that LinkedIn employs commercially reasonable methods to safeguard its user data; (3) provide restitution to Plaintiff and the Class in an amount equal to the Premium Subscription utility paid for but not received; and (4) pay attorney's fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

THIRD CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff and the Class)

129. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

130. In order to purchase a Premium Subscription, Defendant required that Wright affirmatively assent to its Terms of Service, which included LinkedIn's Privacy Policy, and in it, Defendant's representations regarding its security protocols.

131. Plaintiff Wright read the Terms of Service, and with it LinkedIn's Privacy Policy and representations regarding privacy and data security, before initiating her LinkedIn Premium Subscription.

132. Wright assented to the Terms of Service by registering and paying money for a premium account, and thereafter using her LinkedIn Premium Subscription.

133. The Terms of Service constitute a valid and enforceable contract between Plaintiff Wright and LinkedIn governing her LinkedIn Premium Subscription.

134. When Wright agreed to the Terms of Service governing her Premium Subscription, all previous contracts between her and LinkedIn expired, and were superseded and terminated, and thus, an entirely new contract was formed.

135. Wright's Premium Subscription contract was for a single service, which provided LinkedIn's numerous features and functionality along with security protections for her personal and financial information.

136. As part of this Premium Subscription contract, LinkedIn imposed upon itself an obligation to use industry-standard security protocols to protect Wright's personal information.

137. Wright read this representation and considered it in making her decision to purchase a Premium Subscription. Had LinkedIn represented that it would use substandard security measures, Wright would have recognized the Premium Subscription as less useful, and would have either attempted to purchase a Premium Subscription at a lower price or not purchased it at all.

138. Wright performed her obligations under the Premium Subscription contract by paying her subscription fees and abiding by the Terms of Service.

139. By using unsalted SHA-1 protection for its Premium Subscribers' login credentials, LinkedIn breached the term of its contract with Plaintiff Wright to use industry-standard security protocols to protect her personal information.

140. A social networking service with substandard security practices is, in the eyes of the marketplace and consumers such as Wright, a fundamentally less useful and valuable service than a social networking service with industry-standard security protections.

141. Consumers, including social network users, value their privacy. Services, including social networking services, that offer greater data security protections offer consumers greater usefulness and utility than services with substandard security practices. As such, consumers will, if given the choice between two otherwise identical services, choose one with industry-standard security practices over one with substandard security practices.

142. Because of this consumer preference for data security, a social network service with industry-standard security protocols commands a higher market price than a social network service with substandard security protocols.

143. Wright believed she would receive industry-standard protection for her personal information as part of her LinkedIn Premium Subscription, and those security protections were valuable to her.

144. To Wright, the as-promised LinkedIn Premium Subscription offers significantly more utility than the service delivered, which lacked meaningful security protections. Thus, to Wright, the LinkedIn Premium Subscription promised and paid-for was substantially more valuable than the unsecure service delivered.

145. Thus, Wright paid for, but never received, the valuable security protections to which she was entitled, and which would have made her LinkedIn Premium Subscriptions significantly more useful to her.

146. Accordingly, Plaintiff, on behalf of herself and the other Class members, seeks an order declaring that LinkedIn's conduct constitutes breach of contract, and awarding Plaintiff and the Class damages in an amount equal to the difference in the free-market value of the secure services they paid for and the insecure services they received.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Khalilah Wright, individually and on behalf of the Class, prays for the following relief:

A. Certify this case as a class action on behalf of the Class defined above, appoint Khalilah Wright as Class representative, and appoint her counsel as Class counsel;

B. Declare that Defendant's actions, as described herein, violate California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*), and constitute breach of contract;

C. Award injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class members, including, *inter alia*: (i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; and (ii) requiring Defendant to protect all data collected through the course of its business in accordance with industry-standards;

D. Award appropriate damages and restitution to Plaintiff and the Class in an amount to be determined at trial;

E. Award Plaintiff and the Class their reasonable litigation expenses and attorney's fees;

F. Award Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Award such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

Dated: April 30, 2013

KHALILAH WRIGHT, individually and on behalf of all others similarly situated,

By: /s/ Ari J. Scharg
One of Plaintiff's Attorneys

SEAN P. REIS (SBN 184044)
(sreis@edelson.com)
30021 Tomas Street, Suite 300
Rancho Santa Margarita, California 92688
Tel: (949) 459-2124

JAY EDELSON (Admitted *Pro Hac Vice*)*
(jedelson@edelson.com)
RAFEY S. BALABANIAN (Admitted *Pro Hac Vice*)
(rbalabanian@edelson.com)
ARI J. SCHARG (Admitted *Pro Hac Vice*)
(ascharg@edelson.com)
CHRISTOPHER L. DORE (Admitted *Pro Hac Vice*)
(cdore@edelson.com)
EDELSON LLC
350 North LaSalle, Suite 1300
Chicago, Illinois 60654
Tel: (312) 589-6370
*Interim Lead Counsel for Plaintiff and the Putative Class

LAURENCE D. KING (SBN 206423)**
(lking@kaplanfox.com)
LINDA M. FONG (SBN 124232)
(lfong@kaplanfox.com)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Tel: (415) 772-4700
**Liaison Counsel for Plaintiff and the Putative Class

Additional Counsel for Plaintiff and the Putative Class:

JOSEPH J. SIPRUT
(jsiprut@siprut.com)
SIPRUT PC
122 South Michigan Avenue, Suite 1850
Chicago, Illinois 60603
Tel: (312) 588-1440

DAVID C. PARISI
(dcparisi@parisihavens.com)
PARISI & HAVENS LLP
15233 Valleyheart Drive

Sherman Oaks, California 91403
Tel: (818) 990-1299

DAN MAROVITCH
(dmarovitch@marovitchlaw.com)
MAROVITCH LAW FIRM, LLC
233 South Wacker Drive, 84th Floor
Chicago, Illinois 60606
Tel: (312) 533-1605

CERTIFICATE OF SERVICE

I, Ari J. Scharg, an attorney, certify that on April 30, 2013, I served the above and foregoing ***Second Amended Consolidated Class Action Complaint*** by causing true and accurate copies of such paper to be filed and transmitted to all counsel of record via the Court's CM/ECF electronic filing system.

/s/ Ari J. Scharg